

How To Enable Two-Factor Authentication



This article applies to you if you use chimail hosted email (if you log into webmail via chimail.midphase.com)

Two-factor authentication (2FA) is a security measure that requires two separate factors to gain access—something you know and something you have. While it's still important to have a strong, unique password to make it harder to crack ('something you know'), 2FA also incorporates a randomly generated six-digit code that gets sent to or synced with a device you trust like your mobile phone ('something you have').

- [What do I need?](#)
- [How do I enable 2FA on my email account?](#)
 - [Using a Google authenticator](#)
 - [Using SMS messaging](#)
- [Logging in to Webmail with 2FA enabled](#)
- [Disabling 2FA](#)
- [How do I change the authentication method?](#)
- [I lost my 2FA token, how do I get access?](#)

What do I need?

There are a few different ways to get the 2FA code. One of the most common is to use your smartphone with an authenticator app or to have the code sent via text. You can also use password management applications from your computer, like 1Password, to add a 2FA code. All of the options have pros and cons, but some are more severe than others. For example, the authenticator app would need to be disabled or replaced before resetting your phone, but in general, an authenticator app is considered more secure than a text message code which can be diverted to a different device.

Although there are many different authenticator apps that you can use, some authenticator apps that we recommend are:

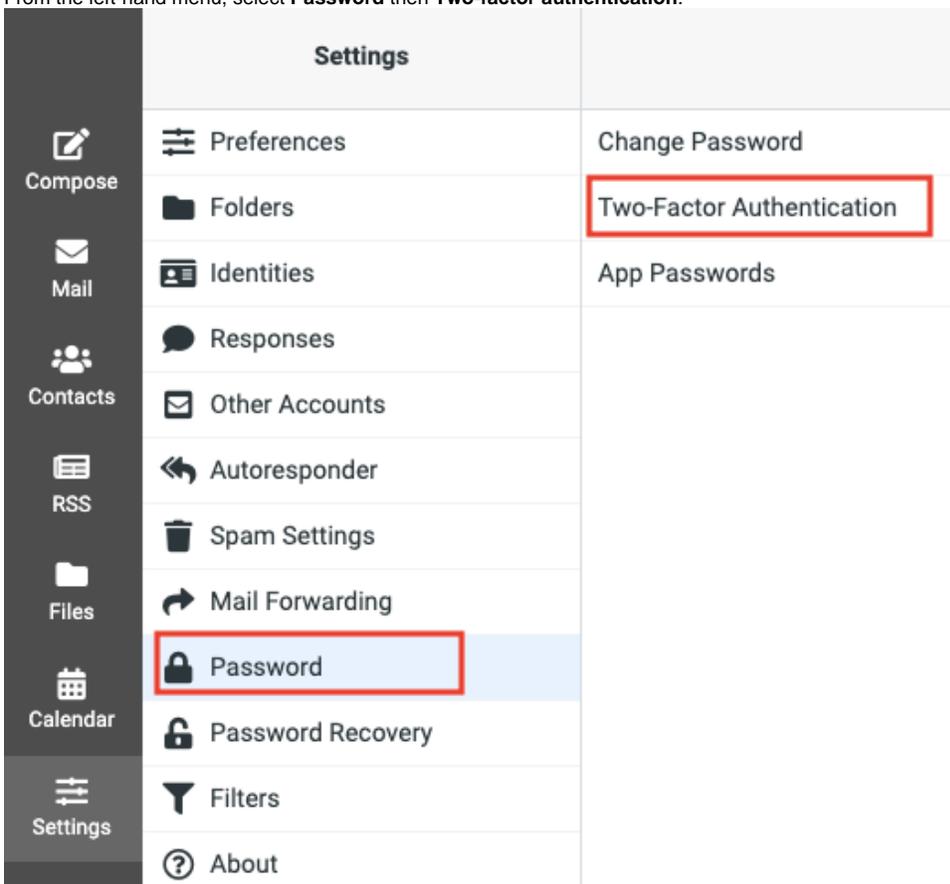
- [Google Authenticator](#) | [iOS](#) | [Android](#) |
- [FreeOTP](#) (Redhat Fork of GoogleAuthenticator) | [iOS](#) | [Android](#) |
- [2 Steps Authenticator](#) ([Blackberry](#))

How do I enable 2FA on my email account?

Using a Google authenticator

1. [Login in to your webmail](#)
2. Select **Settings** from the sidebar

3. From the left-hand menu, select **Password** then **Two-factor authentication**.



4. Choose between setting up 2FA with an authenticator or with SMS text messaging.

Two Factor Authentication is not enabled. Enabling it will increase your account security.

Enable with Google Authenticator

Enable with SMS

5. Select **Enable with Google Authenticator**, and you will be asked to re-enter your password.

Note: Most authenticator apps operate using the same programming principle (TTP) and can be used for 2FA.

Two Factor Auth Enable Phase 1

Please provide your password to continue enabling Google Authenticator.

Current Password

Submit

6. Using your Google Authenticator, scan the QR code and enter in the six-digit code.

Two Factor Auth Enable Phase 2

Google Authenticator (GA) does not require a Google account to use, and no data is sent to Google. Install the GA app or plugin to your mobile device or desktop browser, and scan the QR code below. The app will display a 6 digit verification token; enter it below.



[oma_settings.2fa_url]

otpauth://totp/example@sample.com?secret=x5mhwejdrvkbr

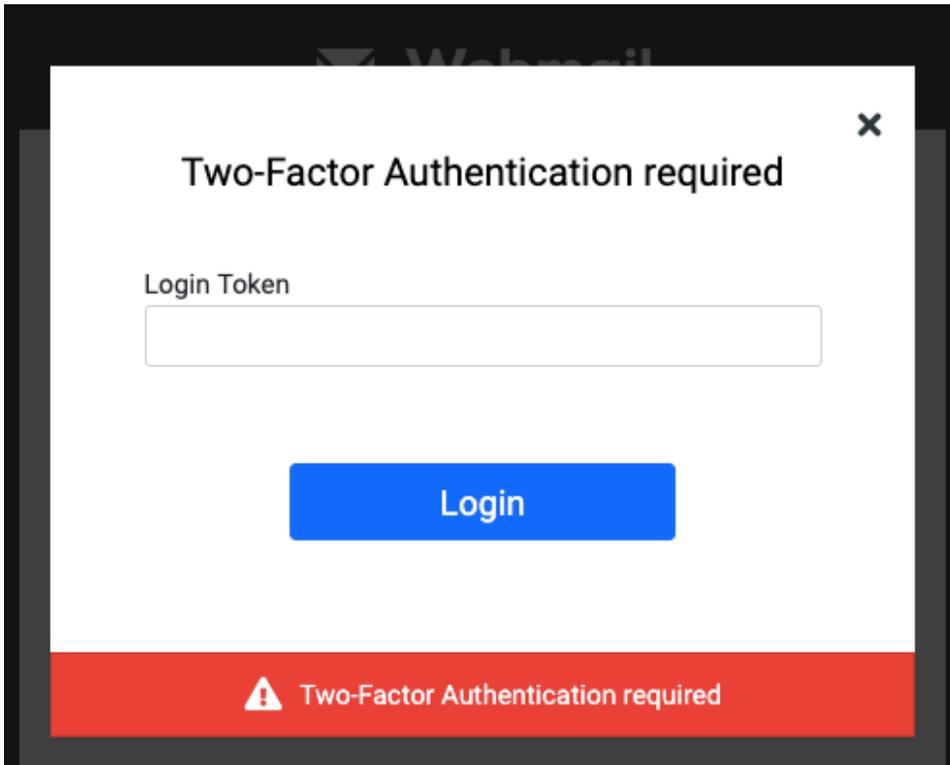
Verification token

Save

7. You will be automatically logged out and when you log back in, two-factor authentication will be required. Your account is now protected by 2FA.

Using SMS messaging

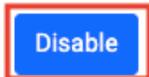
1. [Login in to your webmail](#)
2. Select **Settings** from the sidebar



Disabling 2FA

1. [Login in to your webmail](#)
2. Select **Settings** from the sidebar
3. From the left-hand menu, select **Password** then **Two-factor authentication**.
4. Select Disable.

Two Factor Authentication is enabled on this account using Google Authenticator.

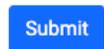


5. Enter your current password and select Submit.

Two Factor Auth Disable Phase 1

You will need to have access to your SMS device or Google Authenticator app in order to disable Two Factor Authentication.

Current Password



6. Enter in your verification token from your SMS or Google Authenticator and click Submit.

Two Factor Auth Disable Phase 2

Obtain a verification token from the Google Authenticator app and enter it below.

Verification token

Submit

7. A confirmation message will appear in the lower corner, and you'll be able to continue without 2FA enabled or [set up a new 2FA device](#).

How do I change the authentication device or phone numbers for 2FA?

To change the authentication method for 2FA, you'll need to log in, disable your 2FA, and re-enable it with the new method.

I lost my 2FA token, how do I get access?

If you've lost your phone, reset it, or replaced it before you were able to disable and reset up 2FA with your new method, you need to [reach out to us](#) to bypass your 2FA authentication. Once it's been bypassed, you will be able to set up 2FA again.

Related articles

- [How To Enable Two-Factor Authentication](#)
- [How To Set Up Email With Your Gmail Account](#)
- [How To Add My Email Account To Entourage](#)
- [How To Add My Email Account To Outlook Express 6.0](#)
- [How To Setup Email In Thunderbird](#)